

SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

Title 10, Code of Federal Regulations, Part 824 (10 CFR Part 824) is the rule published by the Department of Energy (DOE) to implement Section 234B of the Atomic Energy Act of 1954, 42 U.S.C. 2282b. Section 234B stipulates that a contractor or subcontractor to the DOE who violates any rule, regulation, or order relating to the safeguarding or security of Restricted Data, other classified information, or sensitive information shall be subject to a civil penalty (fine) not to exceed \$100,000 per offense. In publishing 10 CFR Part 824, DOE has determined that civil penalties under Part 824 will only be assessed for violations of requirements for the protection of classified information (Restricted Data, Formerly Restricted Data and National Security Information). The rule does not include civil penalties relating to failure to protect other unclassified sensitive information.

SCOPE

This regulation applies to entities that have entered into DOE contracts with DOE, rather than the individual employees of contractors and subcontractors. Contractors and their subcontractors are held responsible for the acts of their employees who fail to observe rules, regulations or orders. *Civil penalties will not be assessed against individual employees.*

Violations of classified information security requirements may be identified and reported through many sources, including: incident reporting and management, security self-assessments, periodic surveys, independent oversight inspections, and Office of the Inspector General and Government Accountability Office activities.

The Security Enforcement staff, within the Office of Security and Safety Performance Assurance (SSA), has primary responsibility for enforcing this regulation as it applies to DOE contractors and subcontractors.

ENFORCEABLE RULES, REGULATIONS AND ORDERS

Currently, violations of requirements to protect classified information found in the following rules and directives could result in 10 CFR Part 824 action:

10 CFR Part 1016, *Safeguarding of Restricted Data* (this rule only applies to Access Permit holders)

10 CFR Part 1045, *Nuclear Classification and Declassification*

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*

DOE M 470.4-2, *Physical Protection*

DOE M 470.4-3, *Protective Force*

DOE M 470.4-4, *Information Security*

DOE M 470.4-5, *Personnel Security*

DOE M 470.4-6, *Nuclear Material Control and Accountability*

SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

In addition, failure to comply with a compliance order issued by the Secretary of Energy dealing with the protection of classified information could be subject to a 10 CFR Part 824 action.

PROCESS

The process outlined in 10 CFR Part 824 is designed to be a comprehensive and fair administrative process that will allow for discussions with the contractor prior to a formal notice of violation which may contain a proposed fine. In the event the Department proposes to fine a contractor, the contractor will always be provided the opportunity to respond and to request a hearing before an Administrative Law Judge.

FACTORS THAT WILL BE CONSIDERED

Violations of classified protection requirements will be assigned a severity level which will be determined based upon an evaluation of the specific facts and circumstances of each case. In addition, a number of other factors will be considered including the frequency and willfulness of the violation(s) and whether appropriate and effective corrective measures have been taken by the contractor to resolve the problem. The rule also provides for reduction of any proposed civil penalty when the contractor has self-reported the violation.

General Summary of the Enforcement Program

Identification

Violations of classified information security requirements may be identified and reported through many sources, including: incident reporting and management, security self-assessments, periodic surveys, independent oversight inspections, and Office of the Inspector General and Government Accountability Office activities.

Security Enforcement staff maintain awareness of all applicable sources and will initiate further assessment and processing where warranted.

Severity Assessment

When a violation is identified, the Security Enforcement staff makes an initial determination of its significance. Three levels of severity are identified:

- Level I is the highest level of violation and is reserved for violations that have an impact on national security.
- Level II violations result from a significant lack of attention or carelessness in protecting classified information.
- Level III violations are those that, if left uncorrected, could lead to more serious concerns.

The severity level is determined based on an evaluation of the specific facts and circumstances of each case. In assigning a severity level, several factors are taken into consideration: the degree of the contractor's responsibility; the training and experience of those involved; past performance of the contractor; and the duration of the violation. A group of violations may be evaluated together and a single severity level assigned.

SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

Investigation

Security Enforcement staff develop further information by means of document reviews, interviews, and other activities. On the basis of this information, the decision is made whether to proceed with further action. This decision takes the same factors into consideration as the assignment of the severity level: the degree of the contractor's responsibility; the training and experience of those involved; past performance of the contractor; and the duration of the violation. A group of violations with the same severity level and similar underlying circumstances may be aggregated for further actions.

Enforcement Conference

After the completion of inquiry or investigation activities and the conclusion that a violation occurred and warrants initiation of the 10 CFR 824 enforcement process, the Director, SSA convenes an Enforcement Conference. This conference is held with Departmental representatives and contractors involved to: ensure the accuracy of facts; discuss the violation and its cause and significance; and present corrective actions and the schedule required for remedial activities. Mitigating or aggravating circumstances and other pertinent information are obtained that will help determine the proper enforcement action.

If DOE determines that the issue's significance is low and the issue does not warrant a notice of violation, DOE issues an enforcement letter that addresses the noncompliance and explains the required corrective actions. DOE then formally closes the enforcement action.

Preliminary Notice of Violation

If DOE determines that a violation warranting 10 CFR Part 824 processing has occurred, the proceedings for imposing a civil penalty begin with a written "preliminary notice of violation," which is sent by certified mail, return receipt requested. This notice contains:

- The facts, nature, and date of each act or omission that constitute the alleged violation.
- The particular provision(s) violated.
- The proposed remedy for each alleged violation, including the proposed civil penalty.
- A statement of the right to reply to the preliminary notice.

DOE uses this notice as a method for formalizing the existence of the potential violation.

Reply

After receiving the preliminary notice, the contractor is required to respond in writing within 30 days. The contractor has several options:

- Admit the violation, waive its right to contest the notice of preliminary violation, and pay the amount assessed.
- Admit the violation but contest the proposed penalty.
- Admit the violation and assert mitigating circumstances that would change the amount of the proposed penalty.
- Deny that the violation occurred and provide justification that the preliminary notice of violation is incorrect.

SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

If the contractor concedes that the violation occurred (i.e., selects one of the first three options listed above), it must describe corrective steps to be taken and the expected results, remedial actions being implemented to prevent recurrence, and the date that full compliance will be achieved.

The written reply must contain a statement of all relevant facts regarding the alleged violation, including:

- Any facts that support the denial.
- Extenuating or mitigating circumstances.
- Authorities (rules, regulations, etc.) that support the position.
- Answers to any questions contained in the preliminary notice.
- Copies of all relevant documents.

DOE then evaluates the contractor's response and makes one of several determinations:

- No violation occurred.
- The violation occurred and the civil penalty should be mitigated either partially or in full.
- The violation occurred and the civil penalty is appropriate (even if mitigating circumstances were asserted).

If the evaluation determines that the violation occurred, a final notice of violation is issued.

Final Notice of Violation

If the DOE final determination finds that the violation occurred or continues to occur, a final notice of violation is issued within 30 calendar days from the time the reply is received. This notice contains:

- The determined violation.
- The amount of civil penalty imposed.
- Further actions necessary or available.
- Notice of a right to request a hearing under Part 824.8.

The notice is deemed final 15 days after it is issued if it does not contain a civil penalty. If it does contain a civil penalty, the contractor must submit one of the following within 30 days of issuance:

- A waiver of further proceedings: The final notice is deemed a final enforceable order. Unless additional time is granted, the penalty set forth must be paid within 60 days of filing the waiver.
- A request for a hearing under Part 824.8: The hearing process is described below.
- A notice of intent to proceed under 234A.c.(3) of the Atomic Energy Act: The civil penalty is assessed, and the procedures of the Act are followed.

Hearing

The procedures for a hearing are specified in 10 CFR Part 824.8, which describes the selection and duties of the hearing counsel and the hearing officer. This section also describes the rights of the contractor to be represented by counsel to be present during the hearing: to testify, present evidence through witnesses or documents, and cross-examine witnesses; and to rebut evidence

SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

and physical records. A transcript of the hearing is made, and appropriate procedures are used to prevent unauthorized disclosure of classified information.

In the hearing, DOE has the burden of proving by a preponderance of evidence that the violation occurred and the proposed civil penalty is appropriate. The contractor has the burden of defending itself against the allegations set forth in the final notice. The hearing officer determines each matter of controversy upon a preponderance of the evidence.

Decision

If the hearing officer determines that a violation has occurred and a civil penalty is appropriate, the initial decision establishes the amount of the civil penalty based on several factors: nature, circumstances, extent, and gravity of the violation(s); violator's ability to pay; effect of the penalty on the contractor's ability to do business; history of prior violations; and degree of culpability. The initial decision includes a notice that it constitutes a final order 30 days after the filing of the decision unless the Secretary files a notice of review.

If the Secretary of Energy files a notice of review, additional proceedings may be conducted, the matter may be remanded, or the civil penalty assessed in the initial decision may be modified. The contractor against which the civil penalty is assessed by the final order shall pay the full amount within 60 days unless DOE agrees otherwise. If payment is not made as required, DOE institutes an action in the appropriate district court to recover the amount of the penalty.

Assessment of Penalty

The civil penalty is a means through which DOE emphasizes the need for compliance with classified information security requirements, emphasizes the necessity of lasting remedial action, and deters future violations. The civil penalty also emphasizes the DOE requirement that contractors identify, report, and take corrective action when violations occur. A civil penalty will be proposed for Severity Level I and II violations, and may be imposed for Severity Level III violations that demonstrate previous corrective actions have failed.

Adjustment Factors

DOE assesses civil penalties to emphasize the importance of compliance with classified information security requirements and to deter future violations. The goal is to ensure that contractors identify, report, and correct deficiencies in their programs before DOE discovers them. DOE therefore takes into consideration the circumstances of each case – considering the promptness, comprehensiveness, appropriateness, timeliness, and initiative displayed by the contractor's corrective action – when offering incentives in the form of adjustment factors.

These adjustment factors may result in a reduced civil penalty for violations promptly identified, reported, and effectively corrected by the contractor. However, if corrective actions are ineffective, or if violations are repeated, flagrant, or indicate a serious breakdown in management controls, the statutory maximum of penalty of \$100,000 per violation per day may be assessed.

DOE normally reduces the amount of the civil penalty when contractors self-identify noncompliance. In evaluating this option, the following factors are considered: time elapsed and number of prior opportunities to identify the violation; effectiveness of contractor control in

SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

preventing or identifying the deficiency; whether the discovery was a result of self-monitoring; extent of DOE involvement in the discovery; and promptness and completeness of reporting. However, DOE does not generally allow a reduction in penalties for self-identification when an event occurs that discloses violations of which the contractor should have been cognizant. The key is whether the contractor should have detected and addressed the noncompliance that contributed to the event.